AMENDMENTS TO THE DRAWINGS

The attached six (6) sheets of replace formal drawings replace the drawings as originally filed. No changes have been made to the content of the drawings, and no new matter has been added.

Attached: Formal Drawings (6 Replacement Sheets)

REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested. Claims 23-26, 32-33 and 38 are canceled, new claims 41-42 are added, and claims 1-22, 27-31, and 34-37 and 39-42 are pending in the application.

Request for Corrected Office Action

Applicant respectfully objects to the Official Action as incomplete because the rejection improperly groups claims 11-22, 26-31, 34-35, and 37-39 as having "similar limitations to claims 1-10, 36, and 40; therefore, they are being rejected under the same rationale." However:

1) claims 1, 10 and 40 were rejected under 35 USC §103 in view of U.S. Patent Publication No. US 2002/0031126 to Crichton and U.S. Patent No. 6,725,371 to Verhoorn, III et al.;

2) claims 2-9 were rejected under §103 in view of Crighton, Verhoorn, III et al., and U.S. Patent Pub. 2003/0093563 by Young; and

3) claim 36 was rejected under §103 in view of Crichton, Verhoorn, III et al., and U.S. Patent No. 7,111,163 to Haney.

As specified in the MPEP, "A plurality of claims should never be grouped together in a common rejection, *unless that rejection is equally applicable to all claims in the group.*" MPEP 707.07(d) at page 700-125 (Rev. 5, Aug. 2006).

Further, Applicant objects to the Office Action is incomplete because it fails to answer all material traversed. See MPEP 707.07(f) at page 700-126 (Rev. 5, Aug. 2006). The statement in the Office Action that "the rejection has been withdrawn" is inadequate, because § 707.07(f) of the MPEP specifically requires the Examiner to address any arguments by the Applicant that are still relevant: "The examiner must, however, address any arguments presented by the applicant *which are still relevant to any references being applied.*" MPEP at 700-127.

Since the Examiner continues to apply Crichton in the §103 rejections, the Examiner has failed to address Applicant's argument that (1) "Crichton et al. does not disclose or suggest the

claimed features of independent claims 1, 10, 18, and 27 that the claimed ***router*** that can reorder a group of data packets 'associated with the corresponding secure connection', as argued on pages 11 and 13 of the Amendment filed February 13, 2007, and that (2) Crichton et al. describes only encryption of a single bitstream having been generated from an analog to digital converter, and neither discloses or suggests a ***router*** outputting to the cryptographic module the "group of data packets, from each corresponding queuing module ***according to the corresponding assigned maximum output bandwidth***".

Hence, a corrected Office Action is requested that (1) properly groups claims according the references being applied; and (2) fully addresses Applicant's arguments that remain relevant regarding the failure of Crichton to suggest the claimed features.

The Independent Claims

Claims 1, 10 and 40 stand rejected under 35 USC §103 in view of U.S. Patent Publication No. US 2002/0031126 to Crichton et al. and Verhoorn, III et al. Based on paragraph 20 of the Official Action, it is presumed that independent claims 18 and 27 also stand rejected under §103 in view of Crichton et al. and Verhoorn, III et al.

This rejection is respectfully traversed, as the rejection fails to establish that "there was an apparent reason to combine the known elements *in the fashion claimed*." *KSR Int'l v. Teleflex, Inc.* No. 04-1350, Slip. op. at 14, 82 USPQ2d 1385, 1396. The rejection has failed to establish the analysis as required by the Supreme Court. Rather, the hypothetical combination teaches no more than "the predictable use of prior art elements according to their established functions," *Id.*, with no disclosure or suggestion of the claimed features as a whole.

Each of the independent claims specify a ***router*** having an outbound interface configured for establishing a plurality of IP-based ***secure connections*** with respective destinations based on respective streams of encrypted packets, where the encrypted packets are ***generated in the router*** by ***a cryptographic module within the router***. Further, supply of data packets to the cryptographic module is controlled by assigning for each secure connection a corresponding queueing module, and ***reordering in each queuing module*** the corresponding group of data

packets according to a determined quality of service policy ***prior to supply to the cryptographic module***.

Hence, latency sensitive traffic can be transported via encrypted tunnels with guaranteed quality of service based on prioritizing the stream of data packets prior to encryption.

As admitted in the rejection, Crichton et al. fails to disclose or suggest outputting to the cryptographic module the group of data packets, from each corresponding queuing module, for generation of the encrypted packets.

Further, the rejection fails to rebut Applicant's argument that Crichton et al. fails to disclose or suggest the claimed features of independent claims 1, 10, 18, and 27 that the claimed ***router*** that can reorder a group of data packets "associated with the corresponding secure connection", as claimed. Further, Crichton et al. describes only encryption of a single bitstream having been generated from an analog to digital converter, and neither discloses or suggests a ***router*** outputting to the cryptographic module the "group of data packets, from each corresponding queuing module ***according to the corresponding assigned maximum output bandwidth***".

Crichton et al. does not teach or suggest a router or a method in a router, as claimed. Rather, Crichton et al. consistently teaches that a **source terminal device** (i.e., a "local device") first generates an encrypted bit stream, and *then* that the encrypted bit stream is output to a "Bit Synchronizer and Internetworker" (BSI) for transmission via a network. For example, Crichton et al. describes at para. 3, lines 10-25 that a prior art secure telephone unit (STU) includes an analog to digital converter for generating a bitstream in response to receiving analog signals from an analog handset microphone: the bitstream is encrypted by a cryptographic module in the STU, and the encrypted bitstream is output by a voice-band modem in the STU to an analog network interface for transmission on a voice network.

Paragraph 5 simply describes that each sequential bit of a bitstream is "exclusively added" by the cryptographic module (i.e., "the encryptor") in the source terminal device to produce in an encrypted bitstream; in other words, paragraph 5 only describes outputting a bitstream to the cryptographic module; as described above with respect to paragraph 2, however, Crichton et al.

describes only encryption of a single bitstream having been generated from an analog to digital converter, and neither discloses or suggests a ***router*** having a cryptographic module.

Moreover, Crichton et al. consistently describes that the *encrypted bitstream* output by the secure source (e.g., 100 of Fig. 1; 1300 of Fig. 13; 1507 of Fig. 15) is received by a local BSI (e.g., 160 of Fig. 1; 1360 of Fig. 13; 1560 of Fig. 15) (see, e.g., para. 18, lines 1-7; para. 51, lines 1-8) and packetized by the local BSI into fixed-size packet payloads (see, e.g., para. 18, lines 7-8; para. 50, lines 5-7; para. 51, lines 15-18; para. 52, lines 1-4): the BSI adds to each fixed-sized packet a "payload sequence number", and the BSI "sends each outbound packet to the outbound transmission path for transmission on a network (e.g., 140 of Fig. 1, 1340 of Fig. 13, 1540 of Fig. 15) as soon as the packet is assembled." (See, e.g., para. 18, lines 8-23; para. 50, lines 5-12; para. 52, especially lines 4-8 and 27-30).

Hence, Crichton et al. consistently describes that the encrypted bit stream output by the secure source is received by the local BSI for creation of packets having payload sequence numbers for transmission on a network. Hence, Crichton et al. neither discloses nor suggests the claimed router performing the "outputting ***to the cryptographic module*** the group of data packets, from each corresponding queuing module ... ***for generation of the encrypted packets***", as claimed, where the outputting to the cryptographic module for generation of the encrypted packets is performed in the router.[1]

Applicant further traverses the citation to claim 22 in Crichton et al. as a teaching of claim 40, as claim 22 of Crichton et al. does not disclose or suggest that the encryption is performed in the router; to the contrary, claim 22 simply specifies that "the system for bit synchronous communications *is used with* ... [an] Internet Protocol router". This is not, however, a teaching that the router includes the cryptographic module, as claimed. Rather, as described in footnote 1 *supra*, the disclosed IP router (1304, 1504) is distinct from the integrated packet

---

[1]Also note in Fig. 15 that the disclosed IP router (1304, 1504) is distinct from the integrated packet secure phone 1505 that includes the crypto module 1507 and the BSI 1560, and that the BSI operations are performed before packets are transmitted to the IP router 1504 (para. 74).

secure phone 1505 that includes the crypto module 1507 and the BSI 1560, and that the BSI operations are performed before packets are transmitted to the IP router 1504 (para. 74).

Crichton et al. also neither discloses nor suggests the claimed router "controlling supply of the data packets ***to the cryptographic module*** by ... ***reordering***, in each queuing module, a corresponding group of the data packets associated with the corresponding secure connection ***according to a determined quality of service policy*** ... and outputting to the cryptographic module the group of data packets, from each corresponding queuing module, ***for generation of the encrypted packets***", as claimed.

Rather Crichton et al. describes that the only reordering is performed by smoothing buffer in the remote BSI (e.g., 160' of Fig. 1, 1360' of Fig. 13, 1560' of Fig. 15) near the destination secure telephone (e.g., 100' of Fig. 1, 1300' of Fig. 13, "1505' of Fig. 15): the smoothing buffer (e.g., 508 of Figs. 5 and 5a) within the packet repair module 206 of the remote BSI reorders the packets received from the packet network (e.g., 140 of Fig. 1, 1340 of Fig. 13, 1540 of Fig. 15) based on the payload sequence number (para. 19, lines 9-14; para. 27, para. 54, lines 1-20; para. 56, para. 59, para. 59, para. 62, para. 68). The remote BSI outputs at synchronous intervals the sequential data from the smoothing buffer in a bitstream to the destination terminal that includes the STU or similar secure device, and locks the output of the smoothing buffer to the timing of the decryptor in the remote terminal (e.g., para. 20, para. 55, lines 15-21).

Hence, Crichton et al. neither discloses nor suggests reordering the group of data packets in a queuing module ***according to a determined quality of service policy***, as claimed, let alone outputting the group of data packets from each queuing module to the cryptographic module ***for generation of the encrypted packets***, as claimed. Rather, Crichton et al. reorders packets after encryption and after having passed through an IP network, in order to restore the packets in their order **according to their sequence numbers**.

Hence, Crichton et al. fails to disclose the claimed features as asserted in the rejection.

As admitted in the rejection, Crichton et al. fails to disclose or suggest outputting to the cryptographic module the group of data packets, from each corresponding queuing module, for generation of the encrypted packets.

Verhoorn, III et al. describes a single queue 210 in a client terminal device (col. 2, lines 50-60) for storing outgoing unsecure packets 213 destined to be output to the network, and incoming secure packets received from the network (see, e.g., col. 3, line 67 to col. 4, line 1 and col. 4, lines 9-11 and 20-26; col. 4, line 65 to col. 5, line 16). There is no disclosure or suggestion in Verhoorn, III et al. for a plurality of queues, as claimed.

Further, Verhoorn, III et al. teaches and incoming provides no reference to a router, as claimed. Consequently, Verhoorn III et al. provides no disclosure or suggestion of performing the encryption in a router, let alone encryption for multiple secure connections, as claimed.

The rejection provides an argument why one skilled in the art would have combined the teachings of Crichton et al. and Verhoorn III et al. *generally* (i.e., according to their predictable use); however, the rejection fails to provide any analysis of any "apparent reason" that one of ordinary skill in the art would have provided any improvements *beyond* (i.e., more than) the predictable use of Crichton et al. and Verhoorn III et al. according to their established functions.[2]

Hence, the hypothetical combination would disclose no more than the secure telephone terminals of Crichton et al. implemented using the secure packet processor of Verhoorn, III et al. There is no disclosure or suggestion of the claimed router performing encryption for multiple secure connections, because this claimed feature provides "more than the predictable use of prior art elements according to their established functions". *KSR Int'l v. Teleflex, Inc.*, Slip op. at 13, 82 USPQ 2d 1385, 1396 (U.S. Apr. 30, 2007).

For these and other reasons, the §103 rejection of the independent claims 1, 10, 18, and 27 must be withdrawn.

It is believed the dependent claims are allowable in view of the foregoing.

In view of the above, it is believed this application is in condition for allowance, and such a Notice is respectfully solicited.

To the extent necessary, Applicant petitions for an extension of time under 37 C.F.R.

---

[2] See *KSR Int'l v. Teleflex, Inc.* No. 04-1350, Slip. op. at 13-14, 82 USPQ2d 1385, 1396.

1.136. Please charge any shortage in fees due in connection with the filing of this paper, including any missing or insufficient fees under 37 C.F.R. 1.17(a), to Deposit Account No. 50-1130, under Order No. 10-008, and please credit any excess fees to such deposit account.

Respectfully submitted,

Leon R. Turkevich
Registration No. 34,035

Customer No. 23164
(202) 261-1059
Date: July 13, 2007